213 #2

Atty. Dkt. No. 068398-0104

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Virgil D. Gligor et al.
Title:	AUTHENTICATION METHOD AND SCHEMES FOR DATA INTEGRITY PROTECTION
Appl. No.:	09/818,608
Filing Date:	03/28/2001
Examiner:	Unassigned
Art Unit:	Unassigned

INFORMATION DISCLOSURE STATEMENT UNDER 37 CFR §1.56

Commissioner for Patents
Washington, D.C. 20231

Sir:

Submitted herewith on Form PTO-1449 is a listing of documents known to Applicants in order to comply with Applicants' duty of disclosure pursuant to 37 CFR §1.56. A copy of each listed document is being submitted to comply with the provisions of 37 CFR §1.97 and §1.98.

The submission of any document herewith, which is not a statutory bar, is not intended as an admission that such document constitutes prior art against the claims of the present application or that such document is considered material to patentability as defined in 37 CFR §1.56(b). Applicants do not waive any rights to take any action which would be appropriate to antedate or otherwise remove as a competent reference any document which is determined to be a *prima facie* art reference against the claims of the present application.

TIMING OF THE DISCLOSURE

The listed documents are being submitted in compliance with 37 CFR §1.97(b), within three (3) months of the filing date of the application.

RELEVANCE OF EACH DOCUMENT

The relevance of the documents is described in the present specification.

Applicants respectfully request that any listed document be considered by the Examiner and be made of record in the present application and that an initialed copy of Form PTO-1449 be returned in accordance with MPEP §609.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741.

Respectfully submitted,

By ______________________

William T. Ellis
Attorney for Applicant
Registration No. 26,874

Date June 28, 2001

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

Page 1 of 1

Form PTO-1449 U.S. DEPARTMENT OF COMMERCE
(MODIFIED) PATENT AND TRADEMARK OFFICE

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

ATTY. DOCKET NO. 068398-0104	SERIAL NO. 09/818,608
APPLICANT Virgil D. Gligor et al.	
FILING DATE 03/28/2001	GROUP ART UNIT Unassigned

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

	A1	GLIGOR et al., "Object Migration And Authentication", *IEEE Transactions On Software Engineering*, Vol. SE-5(6):607-611, (1979)
	A2	MENEZES et al., ""Handbook of Applied Cryptography", pp. 321-367, (1965)
	A3	GILBERT et al., "A Chosen Plaintext Attack Of The 16-Round Khufu Cryptosystem", pp. 340-358, (1988)
	A4	DESMEDT, "Advances In cryptology – CRYPTO '94", 14th Annual International Cryptology Conference, pp. 1-19, (1994)
	A5	BELLARE et al., "Keying Hash Functions For Message Authentication", Springer-Verlag Berlin Heidelberg, pp. 216-233, (1996)
	A6	WIENER, "Advances In Cryptoloty – CRYPTO '99", 19th Annual International Cryptology Conference, pp. 368-383, (1999)
	A7	Federal Information Processing Standards Publication 46-2, Data Encryptioin Standard (DES), pp. 1-5, (1993)
	A8	PETRANK et al., "CBC MAC For Real-Time Data Sources", Federal Information Processing Standards Publication 46-2, Data Encryptioin, pp. 1-18 and 1-23, (1993)
	A9	BELLARE et al., "XOR MACs: new Methods for Message Authentication Using Finite Pseudorandom Functions", pp.1-20 and 1-15, (1995)
	A10	KRAWCZYK, "Advances In Cryptology CRYPTO '98", Springer-Verlag Berlin Heidelberg,pp.265-282, (1998)
	A11	BELLARE et al., "A Concrete Security Treatment of Symmetric Encryption", pp. 394-404, (1996)

EXAMINER	DATE CONSIDERED

* **EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.**